DoD & USMC Public Key Infrastructure (PKI)

Basic Overview

PKI - Basic Overview Introduction

- **Title**: Public Key Infrastructure (PKI) Basic Overview
- **Presentation Mode**: Lecture
- **Prerequisites**: None
- **Classroom Time**: 30 minutes

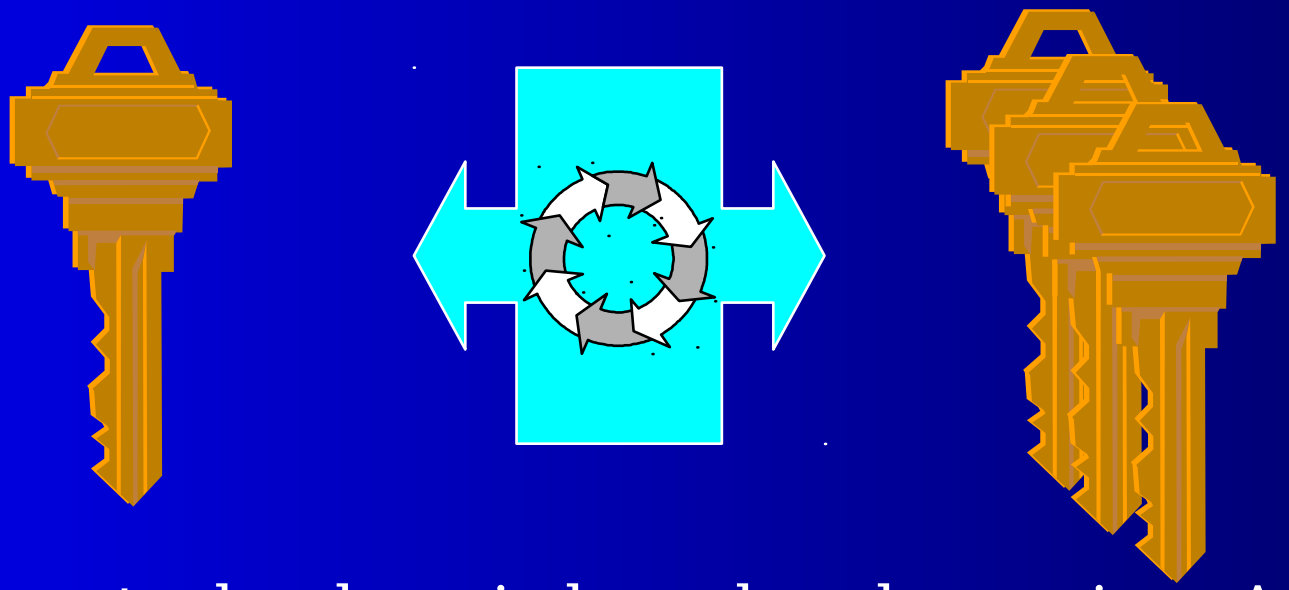
PKI - Basic Overview Learning Objectives

At the end of this lesson, the student will be able to describe:

- Security requirements addressed by using public key encryption and digital signature
- Roles and responsibilities in the PKI process
- Process to create a PKI user account
- Process to generate a public-private key pair and request a certificate
- Process to use a public or private key
- PKI system configuration

Key Pairs

A User's Private Key **A User's Public Key**



Public key technology is based on key-pairs. A user can use their private key to decrypt data encrypted using the corresponding public key. There can be multiple copies of a user's public key, but only one copy of the private key, which is held by the user.

Using Keys

- Keys are used to digitally sign a message and validate this digital signature. A message can be a text or multimedia document.
- Keys are also used to encrypt and decrypt the message.
- A public key can enable access to data encrypted by a corresponding private key. A private key can enable access to data encrypted by a corresponding public key.

Using Keys (cont)

- A public key cannot enable access to data encrypted by the same public key. A private key cannot enable access to data encrypted by the same private key.
- A user retains a private key that he or she uses to send and receive messages. Copies of the user's public key are made available via the directory server.

Using Keys (cont)

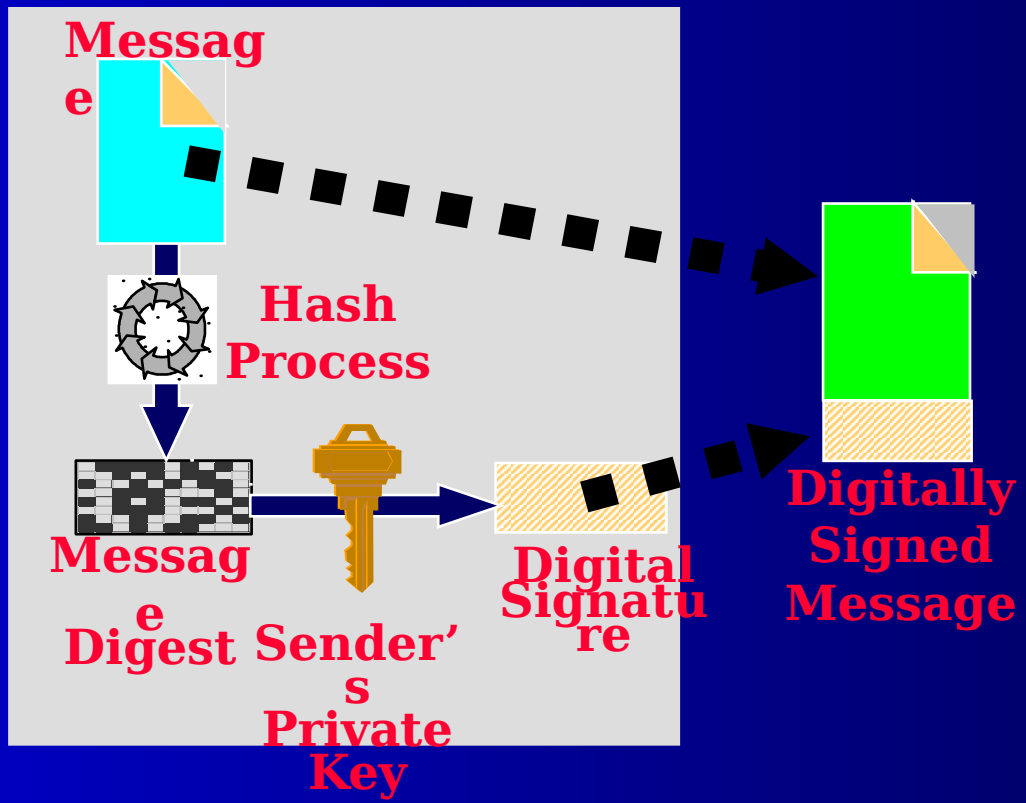
- For example, if Joe needs to verify that Sally has sent a message, or needs to encrypt messages intended only for Sally, Joe can use Sally’s public key to do this. Joe can get a copy of Sally’s public key from the directory server.

Security Requirements Solution

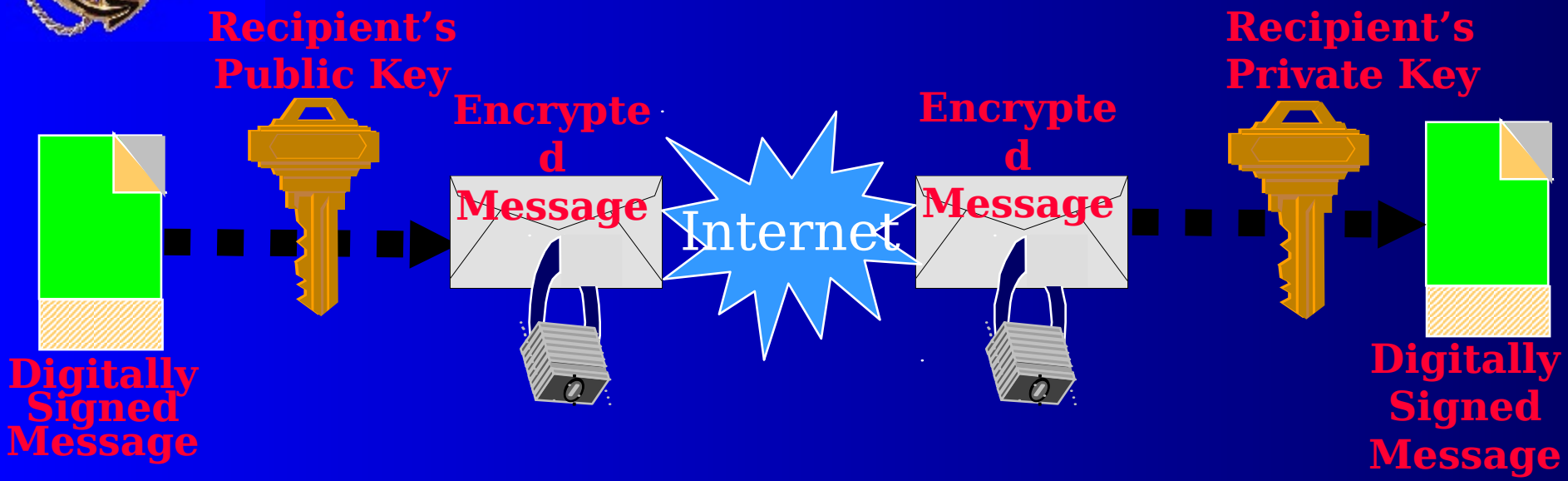
Security Requirements	Security Requirements Definition	Public Keys Satisfy Requirement?
Authentication	Assures that a person or system is exactly who or what they claim to be.	✓
Access Control	Provides access to authorized users while denying access to unauthorized users.	
Data Integrity	Protects against unauthorized changes in data whether they are intentional or accidental.	✓
Confidentiality	Protects against the disclosure of information to unauthorized users. Encryption is typically used to assure confidentiality when information is transmitted over networks.	✓
Non-Repudiation	Protects against a person denying later that a communication or transaction took place as recorded.	✓
Auditing	Monitors intentional or unintentional misuse of security features.	
Availability	Protects against loss of system operation as a result of malicious code, request flooding and penetration attempts	

Non-Repudiation

- The hashing algorithm creates a message digest based on the contents of the message.
- The message digest is then encrypted using the sender's private key and appended to the original



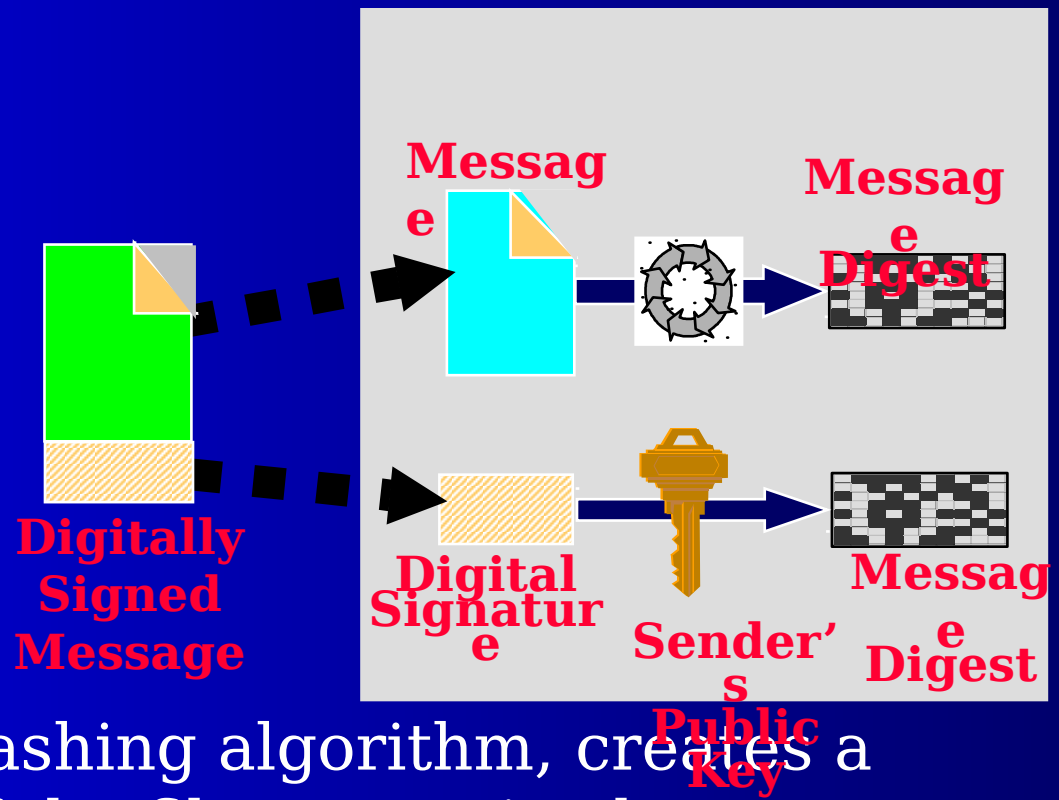
Confidentiality



- The digitally signed message can be encrypted using the recipient's readily available public key.
- This encrypted message is then transmitted via the Internet.
- Once the encrypted message arrives, the recipient will decrypt it using his or her own

Data Integrity

To prove that the received message has not been tampered with during transmission, the recipient does the following:



- Using the same hashing algorithm, creates a message digest of the file as received.
- Using the sender's public key, decrypts the digital signature to view the original message digest.
- Compares the two digests to ensure they are the same.

DoD PKI System Users and System Administrators

Registration Authority (RA) Users

Register LRAs

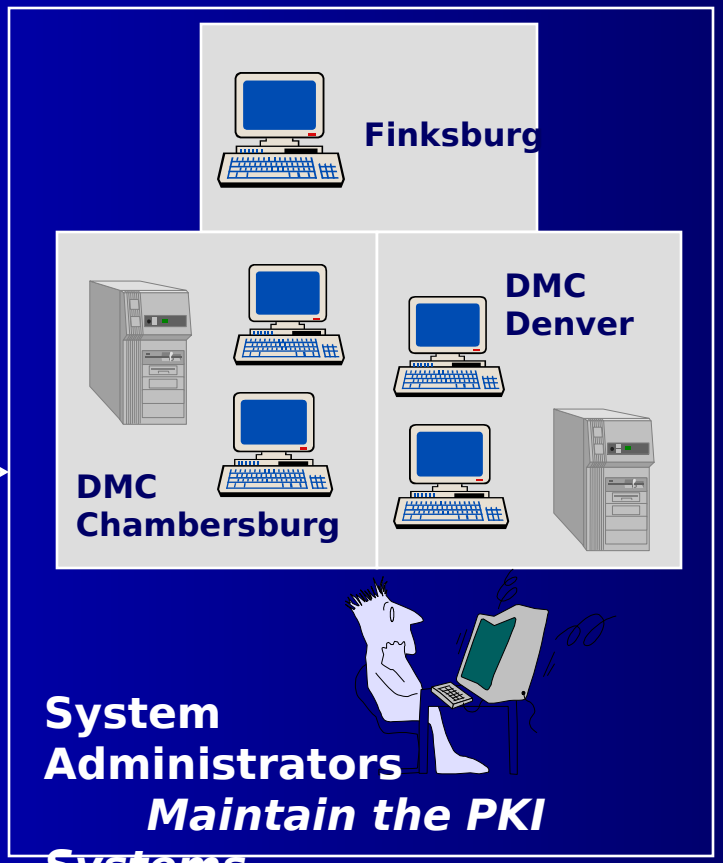
Local Registration Authority (LRA) Users

Register End-Users

End-Users

Acquire Public/Private Keys & Certificates

INTERNET



System Administrators

Maintain the PKI Systems

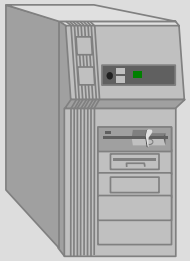
PKI Computer Roles

- **Root CA**
- **Finksburg**

Finksburg

Root Certificate Authority Computer

DMC Chambersburg



Directory Server Master Computer

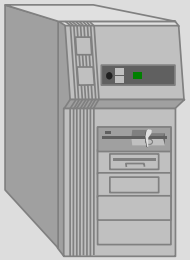
Identity Certificate Authority Computer

E-mail Certificate Authority Computer

DMC Denver

Identity Certificate Authority Computer

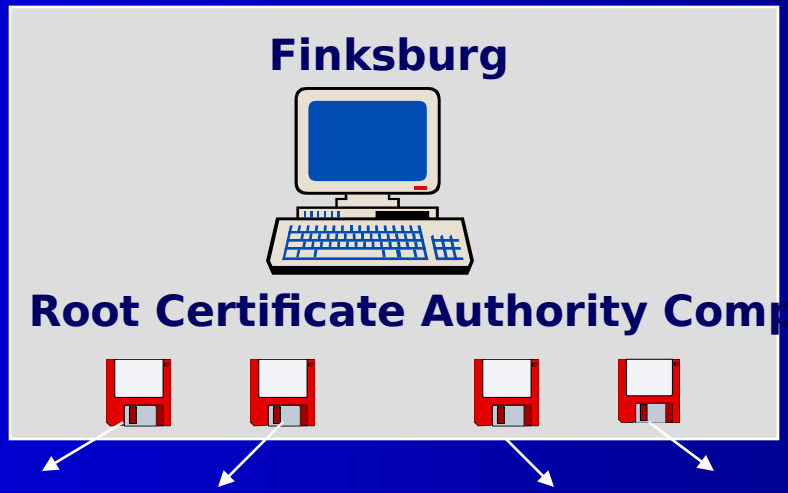
E-mail Certificate Authority Computer

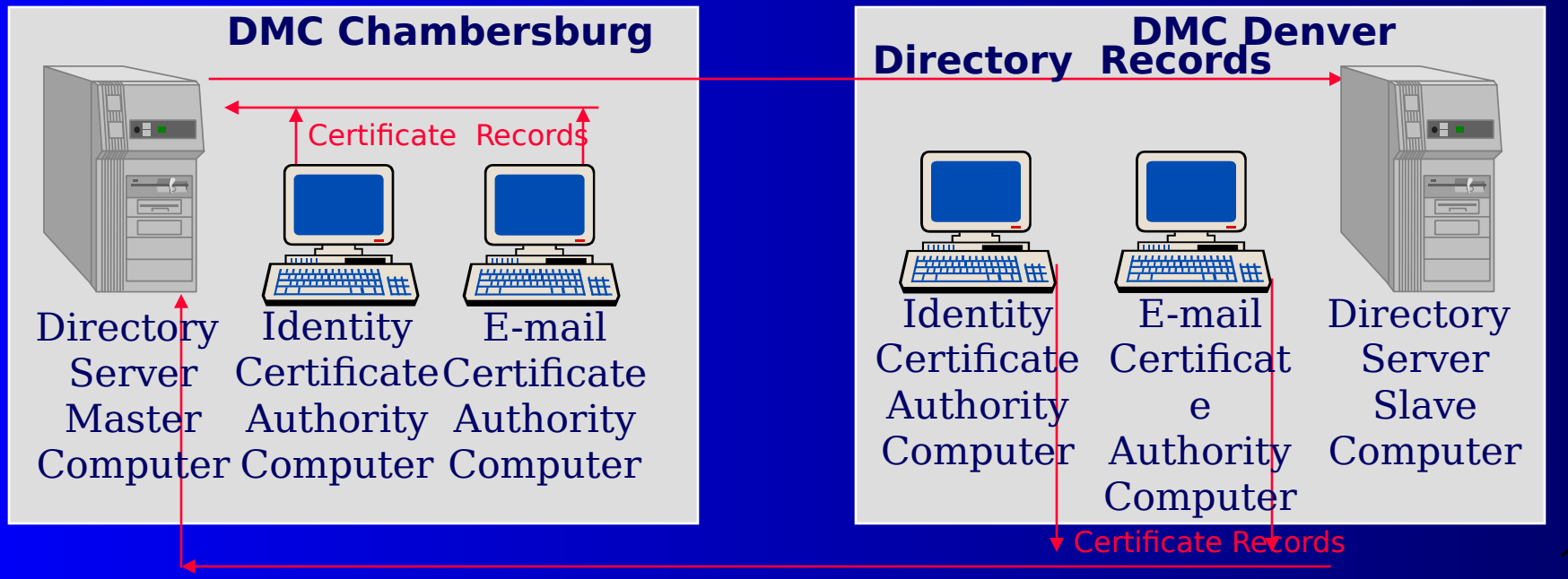


Directory Server Slave Computer

PKI Databases

- **Root CA**
- **Finksburg**



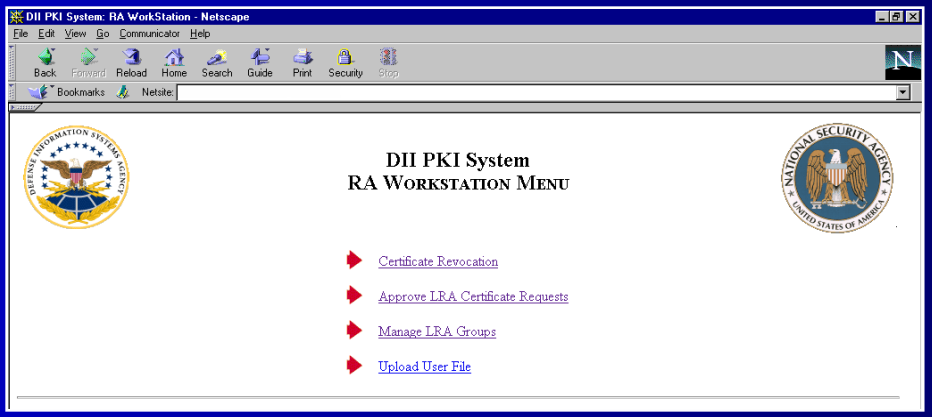


PKI Web Pages

LRA Administration Menu - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Netsite: https://secure.cist.saic.com/lra/
Internet Lookup New&Cool
DII PKI System
LRA Administration Menu
Upload User Data File
Unlock User Account
Open Help Window

https://ca-1-ent.chamb.disa.mil/lra

Identity Certificate Authority Enterprise Webserver


DII PKI System: RA WorkStation - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Netsite:
DII PKI System
RA Workstation Menu
Certificate Revocation
Approve LRA Certificate Requests
Manage LRA Groups
Upload User File

Identity Certificate Authority Computer *at Chambersburg*

https://ca-1-ent.chamb.disa.mil/ra

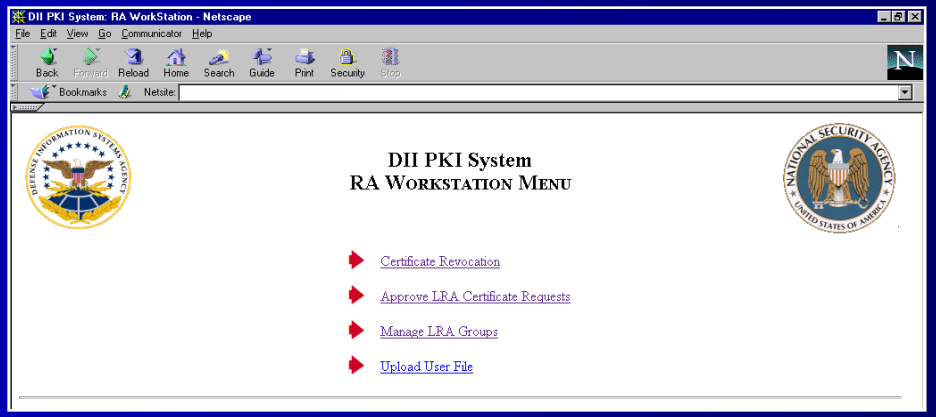
PKI Web Pages (cont)

LRA Administration Menu - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Netsite: https://secure.cist.saic.com/lra/
Internet Lookup New&Cool
DII PKI System
LRA Administration Menu
Upload User Data File
Unlock User Account
Open Help Window

https://ca-2-ent.den.disa.mil/lra

Identity Certificate Authority Enterprise Webserver

Identity Certificate Authority Computer *at Denver*


DII PKI System: RA WorkStation - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Netsite:
DII PKI System
RA Workstation Menu
Certificate Revocation
Approve LRA Certificate Requests
Manage LRA Groups
Upload User File

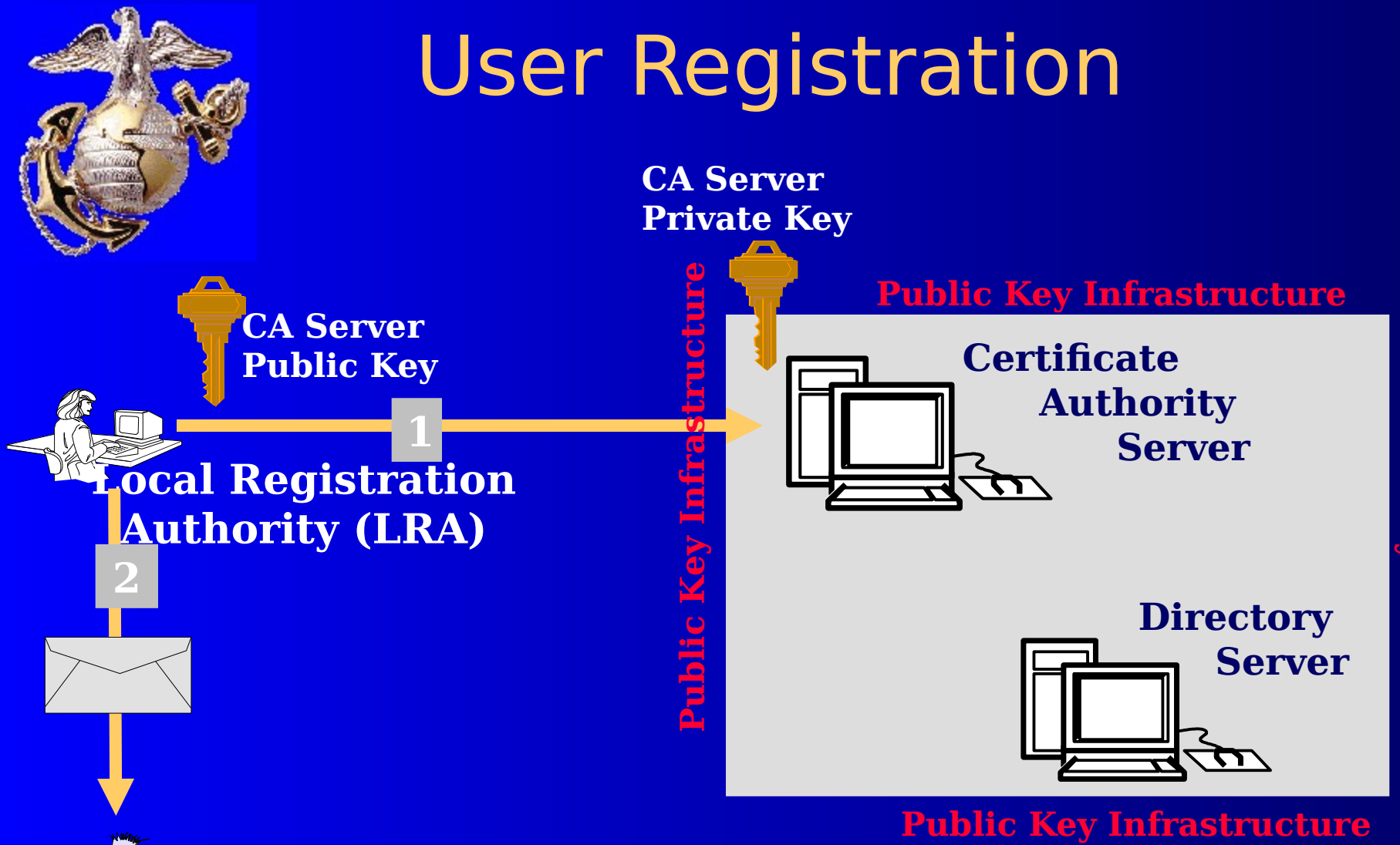
https://ca-2-ent.den.disa.mil/ra

PKI URLs

Computer	Webserver	URL	Initial Web Page
Directory Server	Identity Directory Enterprise webserver	https://ds-1-ent.chamb.disa.mil or http://ds-2-ent.den.disa.mil	DII PKI Homepage
		https://ds-1.chamb.disa.mil/dshtml or http://ds-2.den.disa.mil/dshtml	Netscape Directory Server Screen
Identify Certificate Authority	Identify Certificate Authority webserver	https://ca-1.chamb.disa.mil or https://ca-2.den.disa.mil	Netscape Certificate Server Screen
	Identify Certificate Authority Enterprise webserver	https://ca-1-ent.chamb.disa.mil/ra or https://ca-2-ent.den.disa.mil/ra	DII PKI System RA Workstation Menu
		https://ca-1-ent.chamb.disa.mil/ra or https://ca-2-end.den.disa.mil/lra	DII PKI System LRA Administration Menu
E-mail Certificate Authority	E-mail Certificate Authority webserver	https://e-ca.1.chamb.disa.mil or https://e-ca.2.den.disa.mil	Netscape Certificate Server Screen

- **Chambersburg is the USMC primary site, Denver is secondary.**

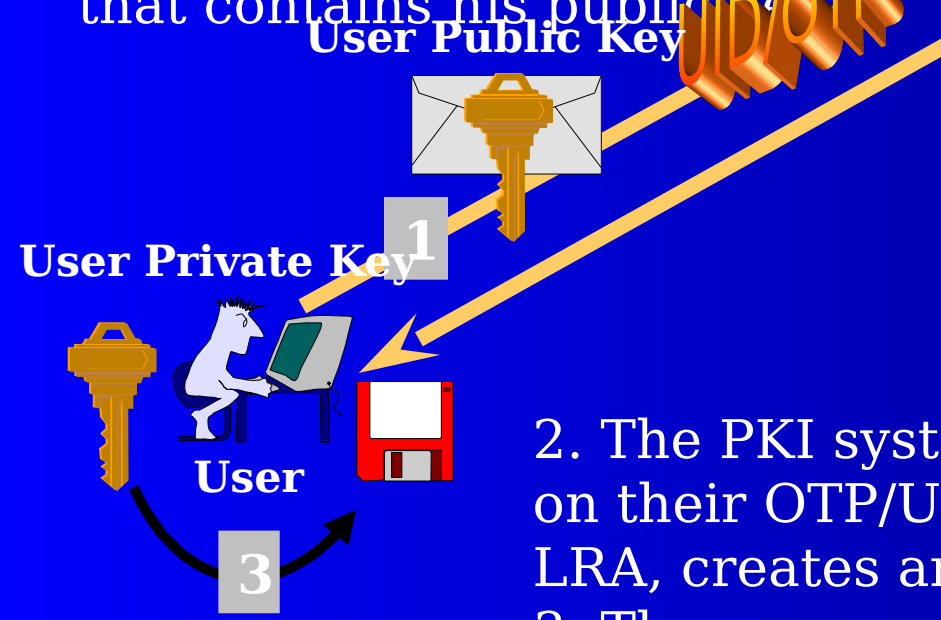
User Registration

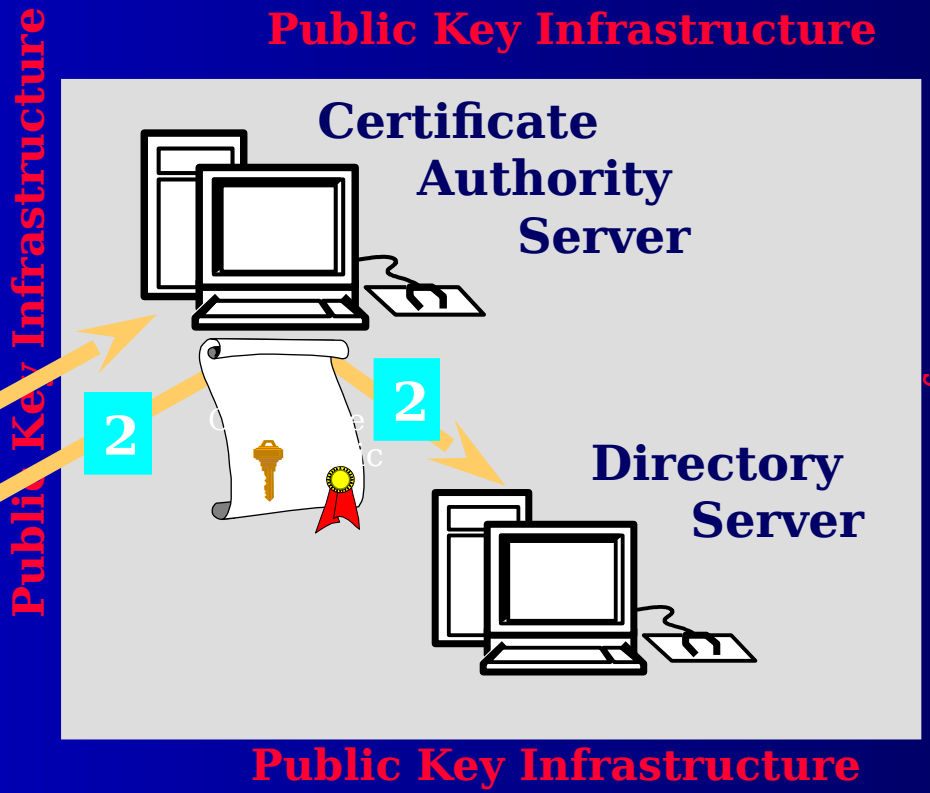


1. Local registration authority (LRA) creates and uploads a user data file.
2. Local registration authority (LRA) provides end user with one-time password (OTP) and 10-digit Unique Identification Number (UIN)

Generating Key Pairs and Certificates

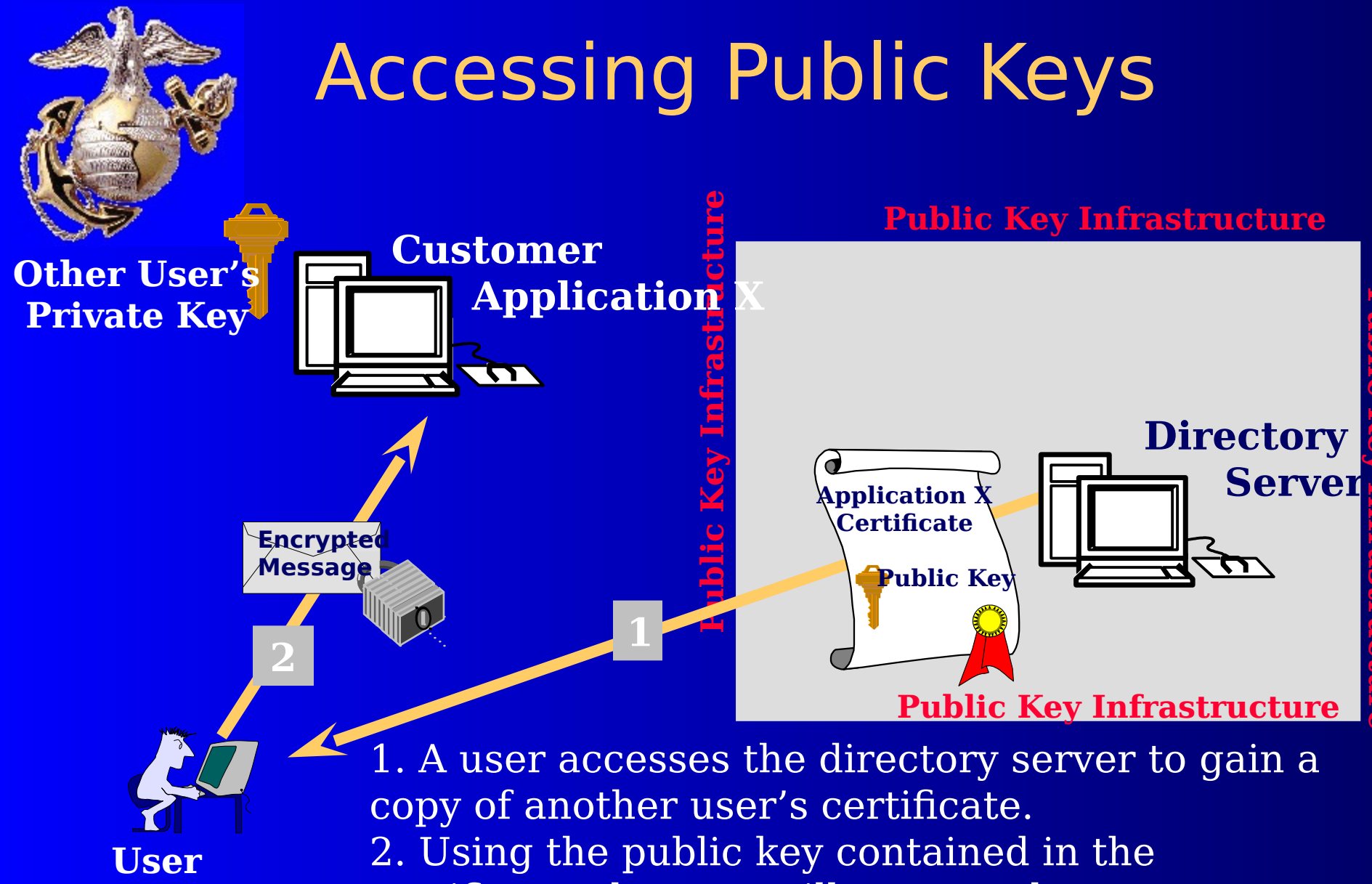
1. A user accesses a web page. Using his OTP/UIN provided by an LRA, the user generates a public-private key pair and submits a certificate request that contains his public key.





2. The PKI system authenticates the user based on their OTP/UID, and with the approval of an LRA, creates and signs the certificate.
3. The user receives and stores the certificate on a removable media.The user also stores his

Accessing Public Keys



1. A user accesses the directory server to gain a copy of another user's certificate.
2. Using the public key contained in the certificate, the user will encrypt the message to ensure confidentiality during transmission. Once received, the message is decrypted using the other

Summary

This lesson has presented an introduction to:

- Security services provided by public/private keys
- Roles and responsibilities in the PKI process
- Process to generate a PKI user account
- Process to generate a public/private key pair and request a certificate
- Process to use a public/private key
- PKI system configuration

Practical Exercise

Directions: Answer the following questions. You may review any class materials for help.

1. Which of the following security services does the use of public key cryptography and digital signatures provide? (Check all that apply)

___ Authentication
___ Access Control
___ Data Integrity
___ Confidentiality
___ Non-Repudiation
___ Auditing
___ Availability

Practical Exercise (cont)

2. Match the person responsible for each of the following activities.

___ Creates an end user account on certificate authority server

___ Generates a public-private key pair

___ Provides user with an OTP/UIN

___ Submits a certificate request for an end user

___ Receives and stores certificate and private key

___ Authorizes LRAs

___ Maintains the PKI system.

A. Local Registration Authority

B. End User

C. System Administrator

D. Registration Authority

Practical Exercise (cont)

3. What does a user need to do to acquire and use private/public keys? (Check all that apply.)

   ___ Acquire a OTP/UIN from a local registration authority.

   ___ Submit a certificate request.

   ___ Store certificate and private key on removable media.

4. How does a user get a copy of another user's certificate that contains their public key? (Check all that apply.)

   ___ Get a copy on a floppy via express mail.

   ___ Access it from the certificate server via the Internet.

   ___ Access it from the directory server via the Internet.

Practical Exercise (cont)

5. Match which key is used in each of the following steps.

___ Applying a digital signature to a message.

___ Encrypting a digitally signed message.

___ Decrypting a digitally signed message.

___ Validating the digital signature on a message.

A. Recipient's public key
B. Sender's public key
C. Recipient's private key
D. Sender's private key

Practical Exercise (cont)

6. Match each of the following items with the place(s) it relates to.

___ Workstation computers	A. Everywhere the PKI system is accessed.
___ Certificate Authority Root	B. Finksburg only
___ Directory server	C. Chambersburg only
___ Identity Certificate Authority	D. Denver only
___ E-mail Certificate Authority	E. Chambersburg and Denver
___ https://ca-1-ent.chamb.disa.mil/lra	
___ https://ca-2-ent.den.disa.mil/ra	

Public Key Infrastructure (PKI)

Basic Overview

END SHOW